## REMARKS/ARGUMENTS

Applicant thanks the Examiner for the interview of June 14, 2005.

The Examiner rejects claims 2, 16, 37, 42, and 44-45 under 35 U.S.C.§102(b) as being anticipated by U.S. Patent 5,774,650 to Chapman et al.; claims 2-7, 10-11, 13-14, 16-20, 23-24, and 26-45 under 35 U.S.C.§102(e) as being anticipated by U.S. Patent 6,516,416 to Gregg et al.; and claims 8-9 and 21-22 under 35 U.S.C.§103(a) as being unpatentable over Gregg et al. in view of Schneier.

Applicant respectfully traverses the Examiner's rejections. Chapman et al., Gregg et al., and Scheier fail to teach or suggest, individually and collectively, at least the following italicized features of the pending independent claims:

> 36. A method of communication data between a first computing device and a second computing device, the method comprising:
>
> (a) a *browser* on the first computing device providing a *Web page* to a user, the *Web page* comprising at least first and second input fields for input from the user and at least a first presentation field associated with the at least first and second input fields;
>
> (b) a program on the first computing device receiving a message from the user, wherein the message comprises at least a first and second datum input by the user into the at least first and second input fields, respectively, of the Web page, wherein the first datum is confidential to the user and the second datum is non-confidential to the user, and *wherein the first datum comprises at least one of a credit card number and a social security number;*
>
> (c) *the program identifying that the first datum is confidential and the second datum is non-confidential;*
>
> (d) *the first computing device communicating, to the second computing device over an untrusted network, the first datum with encryption*; and
>
> (e) *the first computing device communicating, to the second computing device over the untrusted network, the second datum without encryption, wherein steps (d) and (e) occur at least substantially simultaneously.*
>
> 40. A system for communicating data between first and second computing devices, comprising:

(a) a first computer device operable to communicate data over an untrusted network, the first computer device comprising:

a user display, the display comprising at least first and second input fields of a *Web page* for input from the user and at least a first presentation field associated with the at least first and second input fields;

means for receiving a message from the user, wherein the message comprises at least a first and second datum input by the user into the at least first and second input fields, respectively, of the display, wherein the first datum is confidential to the user and the second datum is non-confidential to the user, *wherein the first datum comprises at least one of a credit card number and a social security number*; and

*means for identifying that the first datum is confidential and the second datum is non-confidential*; and

(b) a second communication device in communication with the first communication device, wherein the first computing device communicates, to the second computing device over the untrusted network, *the first datum with encryption and the second datum without encryption.*

44. A method of communicating data between a first computing device and a second computing device, the method comprising the steps of:

at a first computing device, receiving input information from a *Web page* displayed to a user, the input information comprising at least first and second datum corresponding respectively to at least first and second user input fields, *wherein the first datum comprises at least one of a credit card number and a social security number*;

at the first computing device, *a program determining which of the at least first and second user input fields contains confidential information, wherein the first datum is confidential to the user and the second datum is not confidential to the user*;

*the first computing device communicating the first datum of the message to a second computing device with encryption of the first datum*; and

*the first computing device communicating the second datum of the message over an untrusted network to the second computing device without encryption of the second datum.*

45. A data communication system comprising:

(a) a first computer device operable to communicate data over an untrusted network, the first computer device comprising:

a user display, the display comprising at least first and second input fields of a *Web page* for input from the user and at least a first presentation field associated with the at least first and second input fields;

an input operable to receive a message from the user, wherein the message comprises at least a first and second datum input by the user into the at least first and second input fields, respectively, of the display, wherein the first datum is confidential to the user and the second datum is non-confidential to the user and *wherein the first datum comprises at least one of a credit card number and a social security number*; and

*a procedure operable to identify that the first datum is confidential and the second datum is non-confidential;* and

(b) a second communication device in communication with the first communication device, wherein the first computing device communicates, to the second computing device over the untrusted network, *the first datum with encryption and the second datum without encryption.*

The present invention is directed to an encryption module that encrypts only part of a transmission sent by one node to another node. Specifically, a graphical display is presented to a user requesting the user to input information into a number of fields. Some of the fields are confidential while others are not. The fields are identified accordingly. When the user requests transmission of the displayed information to another node, the module encrypts only the confidential fields and not the non-confidential fields. The use of encryption on only part of the transmission can represent substantial savings in computational resources both at the transmitting and receiving nodes.

Chapman et al.

Chapman et al., one of the two primary references, is directed to a method and data processing system for controlling the access of a plurality of users to a computer system connectable over a network to a plurality of computers. The system has facilities for restricting user access to the data processing system which includes a user authentication procedure in which at logon a user's identity is compared with a list of authorized users. In addition, the data processing system has a system-wide profile referenced by all users of the system at logon and temporary access control facilities for temporarily preventing access to the system by a normally

authorized user or users. The temporary access control facilities allow a privileged user of the computer system to create a list of temporarily unauthorized users that is referenced by the system-wide profile at login.

The architecture of Chapman et al. does not involve an untrusted network. Rather, the login communications are communicated over a trusted network (a LAN). The user records used for login use a number of fields, namely a first field 31 giving a unique user's identity or name, a second field 32 for user authentication at login, a third field 33 containing a user number, a fourth field 34 identifies a group to which the user belongs, a fifth field 35 is a text field, a sixth field specifies the user's home directory, and a last field 37 contains the initial program or "shell". At login, the user enters a string at the login prompt, after which the account details are verified. The user's account is validated, the password file 30 is referenced to check that a username 31 exists matching the username supplied by the user, and user authentication 46 performed. In user authentication, the user's identity is verified by comparing the encrypted true password 32 corresponding to the validated username 31 with an encryption of the password supplied by the user who is attempting to gain access. Nowhere does Chapman et al. teach or suggest that the password is the *only* field encrypted during communication of the user inputted login credentials to the UNIX system or that there is any field in the communication of the credentials that is *not* encrypted.

Gregg et al.

Gregg et al., the other primary reference, is directed to a system for controlling the access to computer resources using an untrusted network. The system uses a hardware key connected to each subscriber client computer and adds software to the client computer and to the existing server computer. A clearinghouse is provided to store client and server identification data,

including demographic data, URL data, usage data, and billing information. The clearinghouse authenticates the subscriber and server computers before an operating session occurs. For every new client session, a login mechanism requires the client computer to supply appropriate authentication data, including a digital identification generated by the hardware key. The login parameters are verified by the clearinghouse and a session is then started. The system is adapted to protect a preselected content from being printed or copied by a client using a web browser. The system architecture permits a geographical distributed system of multiple subscriber client computers, multiple server computers and multiple clearinghouses which can interact with one another.

Gregg et al. uses login parameters, namely user name, password, and digital ID, to perform two-factor authentication. (Col. 7, lines 59-65; col. 14, lines 48-58; col. 17, lines 30-37.) Gregg et al. states:

> The subscriber software 36 accepts messages from the web server 69 and takes actions as commanded by the server such as making the subscriber login, polling for the optional access key, *encrypting the login parameters* and sending it to the server, performing URL tracking, and enforcing copyright protection.

(Col. 9, lines 6-12 (emphasis supplied).)

Gregg et al. further states, at col. 13, lines 44-46:

> The login parameters obtained from the user and the access key 54 are encrypted using the challenge sent by the login CGI 68, and sent back to the login CGI 68.

Gregg et al. further states at col. 17, lines 30-37:

> The login interface then sends the login parameters, *including the user name, password, and digital ID* to the client cryptographer (block 148). The client cryptographer encrypts the password and the digital ID using the challenge sent by the login enforcer and sends them to the login enforcer (block 150). The login enforcer then sends an initiate session message to the session initiator with the encrypted login parameters (block 152).

(Emphasis supplied.) Although the Examiner relies on this passage for the teaching that the architecture of Gregg et al. encrypts only the password and digital ID and not the user name, this passage, taken in the context of the other passages, does not teach this. Rather Gregg et al. teach that all of the login parameters are encrypted and sent over the untrusted network. In the above passage, if the user name is not to be encrypted why is it sent to the client cryptographer? It seems clear that all of the login parameters sent to the client cryptographer are encrypted.

Finally, Gregg et al. states at col. 25, lines 50-58:

> In order to perform subscriber authentication, the subscription access server will need to interact with the system clearinghouse 30, which it does by establishing and maintaining a communication line between itself and the clearinghouse. The information transmitted on this communication line is encrypted using a public/private key mechanism so that only authentic servers and an to [sic] authentic subscription access clearinghouse can communicate with each other.

The above references fail to teach or suggest the selective encryption of user inputted information in some fields but not other fields from a common user display when transmitted over an untrusted network.

The dependent claims provide further reasons for allowance.

By way of example, dependent claim 2 requires the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum to include the step of communicating the first datum with encryption and the second datum without encryption in a same packet that comprises the message. *See also* dependent Claims 16, 37, and 42.

Dependent claim 3 requires the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum to include the steps of communicating the first datum

with encryption in a first packet of the message and communicating the second datum without encryption in a second packet of the message different from the first packet of the message. *See also* dependent Claim 17.

Dependent claim 4 requires the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum comprise the step of employing a same path between the first computing device and the second computing device to communicate the first datum with encryption and the second datum without encryption. *See also* dependent Claims 18, 38 and 43.

Dependent claim 5 requires the step of employing the same path to communicate the first datum with encryption and the second datum without encryption to include the step of employing a TCP/IP passage between the first computing device and the second computing device to communicate the first datum with encryption and the second datum without encryption. *See also* dependent Claim 19.

Dependent claim 6 requires the step of communicating the first datum of the message with encryption of the first datum to include the step of employing a key to encrypt the first datum of the message for communication of the first datum from the first computing device to the second computing device with encryption of the first datum. *See also* dependent Claims 7-9 and 20-22.

Dependent claim 10 requires the Web page to include hypertext markup language, the first datum to include the credit card number, the second datum to include information related to a purchase by the user and the program to be embedded in the Web page. The program is loading the program on the first computing device after the Web page is received by the first computing device. *See also* claims 33, 38, and 43.

Dependent claim 41 requires the first and second datum to be communicated at least substantially simultaneously.

Based upon the foregoing, Applicants believe that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

SHERIDAN ROSS P.C.

By: Douglas Swartz

Douglas W. Swartz
Registration No. 37,739
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: June 14, 2005